

AI data handling pre-flight guide

A practical check before you paste, upload, dictate or connect business information to an AI tool.

GENERAL OPERATIONAL GUIDANCE - NOT LEGAL ADVICE

Your obligations depend on the business, people affected, data, provider, contracts and applicable law. Pause and obtain qualified advice where coverage or authority is uncertain.

THE 60-SECOND CHECK

- ☐ What work am I trying to complete - and what information is truly needed?
- ☐ Who owns or may be affected by the information?
- ☐ Is it public, internal, confidential, personal or sensitive?
- ☐ Is the tool and business account approved for that exact use?
- ☐ What happens if the information or output is wrong, exposed or misused?
- ☐ Can I remove identifying detail and use a smaller, safer input?

SAFER DEFAULT

Use the least information, the least identifying detail and the most controlled tool that can complete the task. If you would not put it on a public website, do not use it in an unapproved AI tool without checking first.

Choose the handling path before you share

Use the highest applicable information class. When unsure, choose the more protective path and ask the person responsible for privacy, security or operations.

PROCEED WITH CARE

The information is public or safely generic/de-identified; the business account is approved; no credentials, secrets or unnecessary personal information are included; and a person will check the output before use.

PAUSE AND CHECK

Internal, confidential or personal information is needed; the tool is new or consumer-facing; a contract or client instruction may apply; the output will be sent externally; or you do not understand the provider's data use, access, retention or settings.

STOP AND ESCALATE

Sensitive information, passwords, API keys, payment or identity details, a suspected breach, security vulnerability, complaint, legal dispute, unclear authority, a child or vulnerable person, or a decision affecting employment, credit, insurance, eligibility, safety or legal rights. Do not automate a consequential decision. Obtain designated review and keep a meaningful human override.

INTERNAL CONTROL

The word 'stop' in this guide creates an internal approval control. It does not mean every trigger is a universal statutory prohibition.

Classify and minimise the input

A file can contain more than one class. A simple spreadsheet can contain personal, confidential and sensitive information together. Remove what the task does not need before an AI tool sees it.

CLASS	EXAMPLES	MINIMUM NEEDED	DEFAULT
Public	Published web copy; opening hours	Use only current material	Approved tool; check accuracy
Internal	Process notes; draft plans	Short extract or summary	Approved business account
Confidential	Pricing; contracts; supplier terms	De-identify or do not use	Check authority and terms
Personal	Names; contact details; customer history	Remove identifiers where practical	Check privacy process and purpose
Sensitive / restricted	Health, biometric, identity or security details	Pause by default	Designated approval and safeguards

REPLACE BEFORE YOU PROMPT

- ☐ Use a role or placeholder instead of a name.
- ☐ Use a range, total or category instead of a raw record.
- ☐ Use a short factual extract instead of an entire document.
- ☐ Never include passwords, API keys, account, payment or identity details.

Check the tool before the data enters

Before approving a tool or connection, confirm who can access inputs and outputs, whether data may be used for training, where it is processed, how long it is retained, and whether the business can control access and respond to an incident.

PROVIDER AND ACCOUNT PRE-FLIGHT

- ☐ This is the approved provider, product tier and business account for the task.
- ☐ The provider's access, retention, training/use, deletion, security and incident terms have been reviewed for this use.
- ☐ Only people who need access can use the account, integration or shared output.
- ☐ Data location, overseas access, subprocessors and contractual restrictions are understood before use.
- ☐ A person can pause, disable or fall back from the AI-assisted path if the use changes or fails.
- ☐ The intended output will receive human verification proportionate to the possible impact.

EVIDENCE TO RETAIN FOR HIGHER-RISK USES

1. Provider/product and settings reviewed
2. Purpose, information class and minimisation decision
3. Accountable owner and reviewer
4. Test evidence, decision and next review trigger

PAUSE IF YOU CANNOT ANSWER

Unknown settings, ownership, authority or safeguards are a reason to stop and obtain the right review - not a reason to guess.

Test the use then record the decision

Use representative, de-identified test material first. Do not treat an AI output as verified fact. Check it before it is sent, published or used for a consequential action.

MINIMUM TEST RECORD

TEST CASE	DATA USED	WHAT A PERSON CHECKS	RESULT
Normal	De-identified	Accuracy, completeness and source	Pass / revise
Incomplete	Minimum input	Uncertainty is flagged	Pass / revise
Ambiguous	Generic scenario	No unsupported assumption	Pass / revise
Exception	Safe test case	Pause, escalation and fallback	Pass / revise

SIGN-OFF GATE

No customer message, external publication, purchase, contract, legal or regulated action, material claim or consequential decision should proceed solely from an AI output. Use only safe, de-identified material for a higher-risk test and obtain designated review. Record the owner, reviewer, decision, date and next review trigger.

Continue with the AI Workflow Starter Checklist: praxistra.com/resources/ai-workflow-starter-checklist

Sources: OAIC privacy guidance for commercial AI products; AI.gov.au Guidance for AI Adoption; cyber.gov.au Engaging with AI.